

REMARKS

The present Final Rejection of the claims as anticipated by So is not appropriate. So fails to meet all requirements of the claims as specified inherently by the “if-then” decision carried out in the claims prior to encryption. MPEP 2131 requires that each claim feature must appear in the reference and the elements must be arranged as required by the claim. So fails on both counts. Applicant submits this response in order to avoid the necessity of appeal in this matter and solicits a telephone call from the Examiner to discuss this case upon consideration of the present remarks. Reconsideration and reversal of the present final rejection is respectfully requested as follows.

The So reference describes a method of pre-encryption of content used in a VOD system. So addresses the problem of requirement of a large number of encrypters for real time encryption by use of pre-encryption of the content and ECM retrofitting which apparently only requires that a small quantity of data be changed at the time of demand (see 0017). While So defines selective encryption at 0106, he fails to recognize that selective encryption can be beneficially used as taught by Applicant to reduce the number of encrypters required for real time encryption (i.e., at the time of demand) without need for ECM retrofitting. So’s encryption technique is discussed in the context of there being a large amount of data to be encrypted, and thus, the impracticality of encrypting such large amounts of data on demand without large numbers of encryption devices (see 0014-0017). His solution (ECM retrofitting coupled with pre-encryption) provides an ability to pre-encrypt content using offline encryption facilities that operate once on the content to pre-encrypt it.

There is a fundamental difference between So and Applicant’s claims in that So uses pre-encryption (e.g., see 0017, 0046, 0047), while Applicant’s encryption is carried out on demand (i.e., session based – per the title), as will be explained. Moreover, So teaches against encryption on demand, while Applicant embraces it. Note, for example, at paragraph 0018 So states that his system “includes a content preparation module for pre-encrypting content offline to form pre-encrypted content; an on-demand module receiving the pre-encrypted content ... and forwarding the pre-encrypted content to the subscriber terminal when authorized” (emphasis added). Note also, for example at paragraph 0019, So states that his process involves “pre-encrypting the

content to form pre-encrypted content prior to the step of receiving a request" (emphasis added). Hence, it is clear that So deals with content that has already been encrypted when a request for the content has been received. Moreover, So explicitly states that the content is pre-encrypted so that it only has to be encrypted once.

Not so with Applicant's claimed invention. Contrast So's teachings with the claims (e.g., claim 1 for example without intent to impose limitations) which in part calls for "receiving a request for delivery of the content; determining if the request is from a terminal having decryption capabilities associated with a first decryption method or a second decryption method; if the request is from a terminal having decryption capabilities associated with the first decryption method, then; routing the first portions to a first encryption device; routing the second portions around the first encryption device; encrypting the first portions using a first encryption process at the first encryption device to produce encrypted first portions; and assembling a stream of selectively encrypted content from the encrypted first portions and the second portions." Hence, it is clear that the encryption carried out in Applicant's claims is preceded, predicated and prefaced upon a demand for encrypted content by a requesting terminal. There is no pre-encryption as called for in So.

To highly paraphrase without intent of limitation, Applicant claims that, if the terminal can decrypt using the first decryption method, then selectively encrypt with the first encryption method. Each of Applicant's claims contains such an "if-then" analysis carried out prior to making an encryption method decision. This represents an order of operations that is directly contrary to So's teachings which are, to paraphrase, pre-encrypt, receive request, and retrofit encrypted content for the recipient. If So teaches anything relevant to encryption on demand, it is that it should not be done (see 0014-0017)!

The Examiner asserts that "real time encryption is not a requirement in the claims at hand" (last line of page 5). Applicant notes that the term "real time encryption" is taken from So (first line of 0015) and is construed to mean "encryption on demand". Applicant further notes, that encryption only on demand after making a determination of capabilities of the requesting terminal is clearly a requirement of the claims, and that such is contrary to the pre-encryption and ECM retrofitting as taught by So, and the assertion by the Examiner. So's whole objective is

to move the encryption process forward in the processing cycle so that the number of encryption devices can be minimized by virtue of only encrypting the content once. Applicant seeks to solve a similar problem of reducing the need for large numbers of encrypters, however; Applicant takes advantage of simply pre-processing content to identify content for selective encryption, and then carries out selective encryption when there is a demand (real time). Moreover, the type of encryption used is based upon the capabilities of the requester. This is in stark contrast to So, who teaches that you should pre-encrypts once (see 0017) and avoid real time encryption.

The Examiner notes that So suggests that his system can be used across multiple cable systems. However, Applicant finds no mechanism by which multiple systems can be used simultaneously with multiple encryption techniques. Generally speaking, the encryption techniques used in cable and satellite VOD systems are proprietary (as So acknowledges at 0054) and are thus incompatible with one another. This is well known in the art. As best the undersigned can determine, there is no teaching adequate to overcome these incompatibilities in So by use of his ECM retrofitting and pre-encryption technique. Applicant's technique, however, can be used across multiple systems or in a single mixed system that uses multiple encryption methods since the selective encryption is only carried out on demand (i.e., after it is possible to determine what type of encryption should be used).

In view of the above, it is clear that the current Final Rejection of the claims as anticipated by So is not appropriate. So fails to meet all requirements of the claims in the order specified inherently by the "if-then" decision carried out in the claims prior to encryption. MPEP 2131 requires that each claim feature must appear in the reference and the elements must be arranged as required by the claim. So fails on both counts. Hence, reconsideration and reversal of the present final rejection is respectfully requested.

Concluding Remarks

Per MPEP 2131, to anticipate Applicants' claims the So reference must teach each and every element of the claims in the arrangement called out in the claims. In view of the above, there is clear failure to establish anticipation. Moreover, the So reference clearly teaches away

from techniques that do not use an off-line pre-encryption technique (see, for example, paragraphs 0015-0017). In view of this, not only are the claims not anticipated, they are clearly not rendered *prima facie* obvious by So. Accordingly, reconsideration and allowance are respectfully requested at an early date. The undersigned additionally notes that many other distinctions exist between the cited art and the claims. However, in view of the clear distinctions pointed out above, further discussion of each distinction is clearly unnecessary at this time. Failure to address each point raised in the Office Action should accordingly not be viewed as accession to the Examiner's position or an admission of any sort.

Interview Request

The undersigned sincerely wishes to work with the Examiner to expedite this matter toward allowance, and respectfully requests the courtesy of a telephone interview in order to resolve any outstanding matters and avoid the necessity of appeal in this application.

In view of this communication, all claims are clearly in condition for allowance and such is respectfully requested at an early date.

Respectfully submitted,

/Jerry A. Miller 30779/

Jerry A. Miller
Registration No. 30,779
Dated: 9/25/2006

Please Send Correspondence to:
Miller Patent Services
2500 Dockery Lane
Raleigh, NC 27606
Phone: (919) 816-9981
Fax: (919) 816-9982
Customer Number 24337

Application No.: 10/823,431